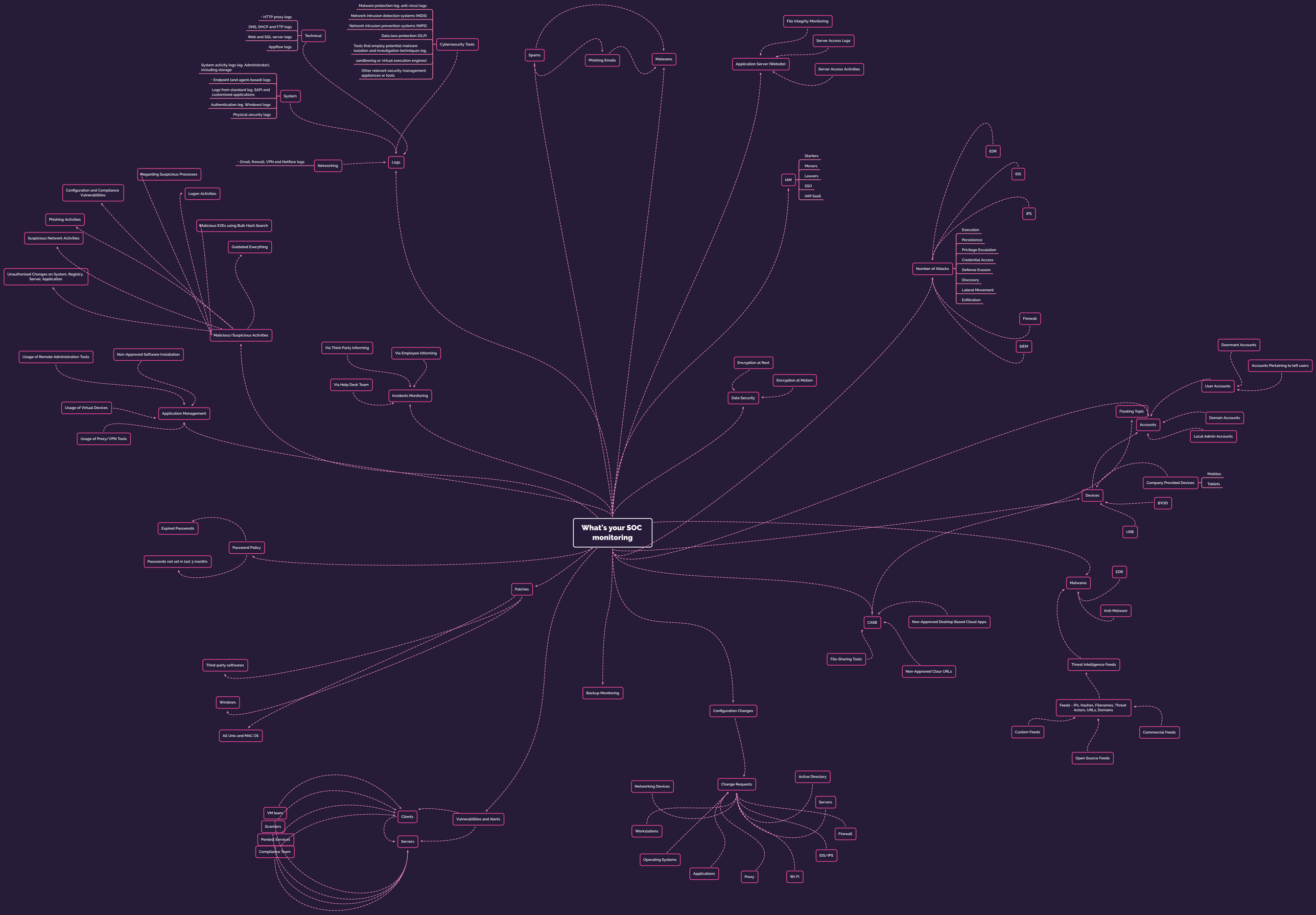
What's your SOC monitoring
Logs
Technical
- HTTP proxy logs
DNS, DHCP and FTP logs
Web and SQL server logs
Appflow logs
Cybersecurity Tools
Malware protection (eg. anti-virus) logs
Network intrusion detection systems (NIDS)
Network intrusion prevention systems (NIPS)
Data loss protection (DLP)
Tools that employ potential malware isolation and investigation techniques (eg.
sandboxing or virtual execution engines)
Other relevant security management appliances or tools
System
System activity logs (eg. Administrator), including storage
- Endpoint (and agent-based) logs
Logs from standard (eg. SAP) and customised applications
Authentication (eg. Windows) logs
Physical security logs
Networking
- Email, firewall, VPN and Netflow logs
Spams
Phishing Emails
Malwares
Application Server (Website)
File Integrity Monitoring
Server Access Logs
Server Access Activities
IAM
Starters
Movers
Leavers
SSO
IAM SaaS
EDR
IDS
IPS
Number of Attacks
Execution
Persistence
Privilege Escalation
Credential Access
Defense Evasion
Discovery
Lateral Movement
Exfiltration
Firewall
SIEM
Malicious/Suspicious Activities
Regarding Suspicious Processes
Configuration and Compliance Vulnerabilities
Logon Activities
Phishing Activities
Malicious EXEs using Bulk Hash Search
Suspicious Network Activities
Outdated Everything
Unauthorised Changes on System, Registry, Server, Application
Usage of Remote Administration Tools
Non-Approved Software Installation
Usage of Virtual Devices
Application Management
Usage of Proxy/VPN Tools
Via Third-Party Informing
Via Employee Informing
Via Help Desk Team
Incidents Monitoring
Encryption at Rest
Encryption at Motion
Data Security
Doormant Accounts
Accounts Pertaining to left users
User Accounts
Floating Topic
Accounts
Domain Accounts
Local Admin Accounts
Company Provided Devices
Mobiles
Tablets
Devices
BYOD
USB
Expired Passwords
Password Policy
Passwords not set in last 3 months
Patches
Third-party softwares
Windows
All Unix and MAC OS
Backup Monitoring
Configuration Changes
Change Requests
Networking Devices
Active Directory
Servers
Workstations
Firewall
IDS/IPS
Operating Systems
Applications
Proxy
Wi-Fi
Clients
Servers
Vulnerabilities and Alerts
VM team
Scanners
Pentest Services
Compliance Team
CASB
Non-Approved Desktop Based Cloud Apps
File-Sharing Tools
Non-Approved Clour URLs
Malwares
EDR
Anti-Malware
Threat Intelligence Feeds
Feeds - IPs, Hashes, Filenames, Threat Actors, URLs, Domains
Custom Feeds
Commercial Feeds
Open Source Feeds